



Laid-Open No.: 2003-0049853

Title: Network protecting system and operation method thereof

Abstract

This research relates to an on-line service providing system and an operation method thereof; and, more particularly, to an invasion detecting system that can detect and shut off any abnormal access to a network smoothly, minimize loss in packet transmission during the operation, build the entire system simply, thus improving the operation speed and security. The service providing method adopting the network protecting system of the present invention includes: a) checking consistently whether a request for session connection between computer systems is received by receiving interrupt signals through an interrupting unit; b) when the request signal for session connection from one computer system to another computer system is generated, controlling data packets transmitted through the session to be transmitted to a kernel; c) determining whether or not the data packet has errors by connecting the kernel with a memory database and determining whether to transmit the data packets to the transmission object computer system or to shut off the data packets the based on the result, and performing according to the determination.

(19)대한민국특허청(KR) (12) 공개특허공보(A)

(51) Int. Cl.⁷
H04L 12/22

(11) 공개번호
(43) 공개일자
특2003-0049853
2003년06월25일

(21) 출원번호
(22) 출원일자
10-2001-0080182
2001년12월17일

(71) 출원인
주식회사 원스텍넷
서울특별시 강남구 삼성동 144-25

(72) 발명자
한대성
경기도남양주시퇴계원면강남전영아파트104-306
신명철
서울특별시관악구신림4동496-23

(74) 대리인
심창섭
김용인

심사청구 : 있음

(54) 네트워크 보호 시스템 및 그 운영 방법

요약

본 발명은 온라인 상의 서비스 시스템 및 이의 운영 방법에 관한 것으로서, 특히, 각종 비정상적인 네트워크 접근의 탐지 및 차단을 위한 과정이 원활히 이루어질 수 있도록 함과 더불어 그 운영에 따른 패킷 전달시의 손실을 최소화하고, 전체적인 시스템의 구축이 간편하게 이루어질 수 있으며, 속도와 안정성의 향상을 이룰 수 있도록 한 침입 탐지 시스템(IDS)을 제공하고자 한 것이다.

이를 위해 본 발명의 네트워크 보호 시스템을 이용한 서비스 방법은 인터럽트부를 이용한 인터럽트 신호의 수신을 통해 각 컴퓨터 시스템간 세션 연결의 요청 여부를 지속적으로 확인하는 제1단계; 상기 과정에서 특정 컴퓨터 시스템으로부터 다른 한 컴퓨터 시스템으로의 세션 연결을 위한 요청 신호가 발생될 경우 이 세션을 통해 전송되는 데이터 패킷을 커널로 전달하도록 제어하는 제2단계; 상기 커널을 메모리 데이터 베이스와 연동시켜 수신된 데이터 패킷의 이상 유무를 판독함과 더불어 그 판독 결과에 따라 전송 대상 컴퓨터 시스템으로의 해당 데이터 패킷 전송 혹은, 차단을 결정하며, 상기 결정에 따른 제어를 수행하는 제3단계:와 같은 일련의 과정이 진행되어 수행됨을 제시한다.

대표도

도 4

색인어

침입 탐지 시스템, IDS 커널, 메모리 데이터 베이스(MDB)

명세서

도면의 간단한 설명

도 1 은 종래 침입 탐지 시스템이 구축된 네트워크를 개략적으로 나타낸 구성도

도 2 는 본 발명에 따른 침입 탐지 시스템이 구축된 네트워크 보호 시스템을 개략적으로 나타낸 구성도

도 3 은 본 발명에 따른 침입 탐지 시스템의 IDS 커널과 메모리 데이터 베이스 상호간 연동 구성을 개략적으로 나타낸 구성도

도 4 는 본 발명에 따른 침입 탐지 시스템이 구축된 네트워크 보호 시스템의 운영 과정을 개략적으로 나타낸 순서도

도 5 는 본 발명에 따른 침입 탐지 시스템의 IDS 커널과 메모리 데이터 베이스 상호간 연동에 따른 침입 탐지 및 방어를 수행하는 과정에 대하여 간략히 나타낸 순서도

도 6 은 도 5의 운영 과정 중 IDS 커널의 분석 프로세서가 운영되는 과정을 간략히 나타낸 순서도

도 7 은 도 5의 운영 과정 중 IDS 커널의 방어 프로세서가 운영되는 과정을 간략히 나타낸 순서도

도 8 은 도 5의 운영 과정 중 IDS 커널의 추적 프로세서가 운영되는 과정을 간략히 나타낸 순서도

도 9 는 도 5의 운영 과정 중 IDS 커널의 경고 프로세서가 운영되는 과정을 간략히 나타낸 순서도

도 10 는 도 5의 운영 과정 중 IDS 커널의 로깅 프로세서가 운영되는 과정을 간략히 나타낸 순서도

도면의 주요부분에 대한 부호의 설명

100. 침입 탐지 시스템(IDS) 120. 인터럽트부

130. IDS 커널 131. 패킷 수집 프로세서

132. 분석 프로세서 133. 방어 프로세서

134. 관리 프로세서 135. 경고 프로세서

136. 추적 프로세서 137. 로깅 프로세서

138. 패킷 전송 프로세서

160. 메모리 데이터 베이스(MDB) 170. 데이터 버스

180. HDD 190. 유저 인터페이스(UI)

200. 허브

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 온라인 상에서 특정 네트워크 내부로의 비정상적인 침입을 방지할 수 있도록 함과 더불어 해당 네트워크 내부의 컴퓨터 시스템을 이용한 비정상적인 사용, 오용, 남용 등을 방지할 수 있도록 한 시스템 및 이의 운영 방법에 관한 것이다.

현재, 인터넷(internet) 환경의 급격한 발달로 인해 각 개인은 필요로하는 정보를 인터넷 환경 내에서 자유롭게 취득하거나 전송할 수 있게 되었고, 각 기업체에서도 원거리 상에 위치되어 있다 하더라도 상기한 인터넷을 통해 각종 자

료의 공유가 가능하게 되었다.

하지만, 상기한 바와 같이 각종 정보가 인터넷 환경 내에서 자유롭게 전달 및 취득이 가능함에 따라 각 개인 정보의 오용 및 남용이 급증하게 되었을 뿐 아니라 특히, 각 기업체에서는 중요한 정보 데이터의 유출이 증가됨에 따라 보안의 중요성이 점차 대두되고 있다.

이에 최근에는 IDS(Intrusion Detection System)와 같이 인가되지 않은 시스템으로부터의 접속을 차단하기 위한 침입 방지 시스템을 각 네트워크 상에 설치함으로써 정보의 유출을 최대한 방지할 수 있도록 하고 있다.

이 때, 상기 IDS는 각 네트워크간의 통신에 직접 관여하는 것이 아니라 특정 네트워크간 통신 세션의 발생시 이 세션을 모니터링하는 패시브(passive) 방식을 채택하고 있다.

즉, 상기 IDS는 별도의 서버로 네트워크에 포함되어 구축된 상태로써 인터넷을 통해 외부 네트워크와 접속한 네트워크 내부의 각 시스템간 세션을 지속적으로 모니터링 하여 상기 세션을 통해 통신되는 각 데이터의 이상 발생 유무를 확인하여 이상이 있을 경우 해당 세션을 강제 차단하도록 운영되기 때문이다.

하지만, 상기와 같은 기존의 IDS는 특정 시스템의 OS(Operating System) 상에 설치되는 응용 프로그램(Application Program)임을 고려할 때 전체적인 처리 속도가 늦고, 침입 탐지 과정 중의 패킷 손실이 많았던 문제점이 있다.

예컨대, 도시한 도 1과 같이 IDS 애플리케이션(11)이 설치된 시스템(10)은 인터럽트부(12)를 이용하여 각 허브(20)에 연결되어 있는 각 컴퓨터 시스템의 인터럽트 신호를 감시하는 도중 특정 컴퓨터 시스템간 세션 접속이 이루어질 경우 상기 접속된 세션간의 전송 데이터 패킷을 확인하여 커널(13)을 통해 네트워크 드라이버(driver)(14)로 전달하고, 상기 네트워크 드라이버(14)는 상기 IDS 애플리케이션(11)을 통해 해당 데이터 패킷의 이상 발생 여부를 판독하게 된다.

이의 과정에서 네트워크 인터페이스 카드(Network Interface Card)(15)와 같은 디바이스를 통해 데이터 패킷을 전달받은 커널(13)이 네트워크 드라이버(14)의 데이터 패킷을 전송하는 도중 및 네트워크 드라이버(14)가 IDS 애플리케이션(11)으로의 데이터 패킷을 전송하는 도중 처리 속도의 저하와 함께 상당수의 패킷 손실이 발생하게 된다.

즉, IDS에 의한 침입 탐지의 전반적인 과정이 데이터의 이동에 따름에 따라 커널(kernel)(13)에 의한 데이터 전달 과정에서의 병목현상이 발생하는 등 처리 속도의 한계를 가질 수 밖에 없었을 뿐 아니라 패킷 전달 과정에서의 많은 손실이 발생하여 해당 데이터를 검사하지 못하는 가장 큰 문제점이 있다.

또한, 상기와 같은 통상적인 IDS는 그 동작 중 특정 시스템간의 비정상적인 세션 연결을 확인하게 될 경우 상기 세션 연결된 각 시스템에 방어 패킷을 동시에 보냄으로써 상호간의 세션을 차단하게 되는데, 이의 과정이 상당한 정확도를 가져야만 하였던 기술적인 어려움이 있었다.

특히, 기존의 IDS는 여타 네트워크와의 세션 접속이 이루어진 상태로 그 모니터링이 수행되고, 상기 모니터링 과정에서 이상이 발견될 경우 상호간의 세션을 차단하도록 제어됨에 따라 서비스 거부 공격(DOS; Denial Of Service) 및 분산 서비스 거부 공격(DDOS; Distributed Denial Of Service)과 UDP(User Datagram Protocol)를 이용한 해커의 공격에 취약하였던 문제점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 전술한 바와 같은 종래 문제점을 해결하기 위해 안출한 것으로서, 각종 비정상적인 네트워크 접근의 탐지 및 차단을 위한 과정이 원활히 이루어질 수 있도록 함과 더불어 그 운영에 따른 패킷 전달시의 손실을 최소화하고, 전체적인 시스템의 구축이 간편하게 이루어질 수 있으며, 속도와 안정성의 향상을 이룰 수 있도록 한 침입 탐지 시스템(IDS)을 제공하는데 그 목적이 있다.

발명의 구성 및 작용

상기한 목적을 달성하기 위한 본 발명의 형태는 인터넷 망을 통해 연결된 특정 영역 외부에 구축된 네트워크의 컴퓨터 시스템 및 특정 영역 내부에 구축된 네트워크의 특정 컴퓨터 시스템간 혹은, 특정 영역 내부에 구축된 네트워크의 각 컴퓨터 시스템간 데이터 전달을 위해 설치된 최소 하나 이상의 허브; 상기 특정 영역 내부에 구축된 네트워크망을 이루며, 각 허브에 접속된 상태로써 네트워크링 가능하게 연결된 다수의 서버 컴퓨터 시스템 및 개인용 컴퓨터 시스템; 상기 각 허브 중 어느 한 허브와 이 허브에 연결된 다른 한 허브 혹은, 컴퓨터 시스템과의 데이터 전달 경로 사이에 최

소 하나 이상 설치되며, 상기 데이터 전달 경로 사이의 데이터 전달에 대한 인터럽트 신호를 수신받아 침입 탐지 및 방어를 수행하도록 침입 탐지 엔진이 모듈화되어 이루어진 커널(kernel)을 가지는 침입 탐지 시스템(IDS:Intrusion Detection System)을 포함하여 구축된 네트워크 보호 시스템을 제시한다.

그리고, 상기한 형태에 따른 본 발명의 운영 방법으로 인터럽트부를 이용한 인터럽트 신호의 수신을 통해 각 컴퓨터 시스템간 세션 연결의 요청 여부를 지속적으로 확인하는 제1단계; 상기 과정에서 특정 컴퓨터 시스템으로부터 다른 한 컴퓨터 시스템으로의 세션 연결을 위한 요청 신호가 발생될 경우 이 세션을 통해 전송되는 데이터 패킷을 커널로 전달하도록 제어하는 제2단계; 상기 커널을 메모리 데이터 베이스와 연동시켜 수신된 데이터 패킷의 이상 유무를 판독함과 더불어 그 판독 결과에 따라 전송 대상 컴퓨터 시스템으로의 해당 데이터 패킷 전송 혹은, 차단을 결정하며, 상기 결정에 따른 제어를 수행하는 제3단계:가 포함되어 진행되는 방법을 제시한다.

이하, 첨부된 도면을 참조하여 본 발명의 네트워크 보호를 위한 시스템 및 그 운영 방법에 관한 실시예를 도시한 도 2 내지 도 10을 참고로 하여 보다 상세히 설명하면 다음과 같다.

우선, 첨부된 도 2는 본 발명의 네트워크 보호를 위한 시스템을 개략적으로 나타내고 있다.

즉, 본 발명의 네트워크 보호 시스템은 크게 네트워크에 연결된 다수의 컴퓨터 시스템(300)과, 상기 각 컴퓨터 시스템간의 데이터 전달을 위한 최소 하나 이상의 허브(200)와, 각 컴퓨터 시스템간에 전달되는 데이터의 이상 유무를 판독하여 이상이 있는 데이터는 차단하고, 이상이 없는 데이터만을 전송 대상 컴퓨터 시스템으로 전달하도록 구축된 침입 탐지 시스템(IDS:Intrusion Detection System)(100)을 포함하여 구축된다.

상기에서 네트워크 보호 시스템을 구성하는 각 컴퓨터 시스템(300)은 특정 영역 내부에 구축된 네트워크 망을 이루며, 각 허브(200)에 접속된 상태로써 네트워크 가능하게 연결되고, 각 컴퓨터 시스템(300)간의 제어나 메일과 같은 여타의 작업을 수행하기 위한 다수의 서버 컴퓨터 시스템과 각각의 개인이 사용하는 개인용 컴퓨터 시스템으로 구성된다.

그리고, 상기 허브(200)는 특정 컴퓨터 시스템으로부터 인터넷 망이나 인트라넷 망을 통해 전송되는 데이터를 입수하여 상기 데이터의 전송 대상 컴퓨터 시스템(300)으로 전달하는 역할을 수행하게 되며, 라우터의 기능을 포함할 수도 있고 그렇지 않을 수도 있다.

이 때, 상기 허브(200)가 라우터 기능을 포함하지 않을 경우에는 도시된 바와 같이 상기 허브(200)와 인터넷망 사이에 별도의 라우터(400)를 구비하여야 함은 당연하다.

그리고, 상기 네트워크 보호 시스템을 구성하는 허브(200)는 인터넷 망을 통해 연결된 상태로써 특정 영역 외부에 구축된 네트워크의 컴퓨터 시스템(예컨대, 개인용 PC 등) 및 특정 영역 내부에 구축된 네트워크의 특정 컴퓨터 시스템 혹은, 특정 영역 내부에 구축된 네트워크의 각 컴퓨터 시스템간 데이터 전달을 위해 설치된다.

그리고, 상기 네트워크 보호 시스템을 구성하는 침입 탐지 시스템(100)은 네트워크를 이루는 각각의 허브(200) 중 어느 한 허브와 이 허브에 연결된 다른 한 허브 혹은, 컴퓨터 시스템(300)과의 데이터 전달 경로 사이에 최소 하나 이상 설치된다.

이 때, 상기 침입 탐지 시스템(100)은 상기 데이터 전달 경로 사이의 데이터 전달에 대한 인터럽트 신호를 수신받아 침입 탐지 및 방어를 수행하도록 침입 탐지 엔진이 모듈(module)화된 커널(Kernel 이하, "IDS 커널"이라 한다)(130)과, 네트워크 망에 접속된 상태로써 데이터의 송수신을 위한 네트워크 인터페이스 카드(NIC:Network Interface Card, 이하, NIC라 한다)(150)와, 상기 NIC를 통한 데이터의 수신 여부에 따른 인터럽트(Interrupt) 신호를 판독하는 인터럽트부(120)와, 상기 IDS 커널(130)을 통해 수신되는 각 데이터 패킷을 임시 저장하고, 각 패킷의 이상 현상에 대한 정보 및 각 패킷의 이상 상태별 대응 방법에 대한 제어 정보가 각각 저장되는 메모리 데이터 베이스(MDB:Memory Data Base, 이하, MDB라 한다)(160)와, 상기 각 구성 부분간의 데이터 전송이 이루어지도록 연결된 데이터 버스(Data Bus)(170)를 포함하여 구성된다.

즉, 본 발명은 침입 탐지 시스템의 침입 탐지 및 방어를 위한 엔진을 모듈화된 IDS 커널(130)로써 구현한 것이다.

그리고, 상기 IDS 커널(130)은 크게 패킷 수집 프로세서(Gathering Processor)(131)와 분석 프로세서(Analyze Processor)(132), 방어 프로세서(Defense Processor)(133), 관리 프로세서(Manager Processor)(134)로 이루어진다.

이 때, 상기 패킷 수집 프로세서(131)는 인터럽트부(120)를 통해 데이터의 수신 여부가 확인될 경우 해당 데이터 패킷을 지속적으로 받아들여 MDB(160)에 저장하는 역할을 수행한다.

그리고, 상기 분석 프로세서(132)는 상기 MDB(160)에 저장되어 있는 각 데이터 패킷을 분석하여 그 이상 유무를 판독하고, 그 결과 정보를 상기 MDB(160)에 재 저장하는 역할을 수행한다.

그리고, 상기 방어 프로세서(133)는 상기 MDB(160)에 저장된 각 데이터 패킷의 이상 유무에 따른 정보를 토대로 선택적으로 방어하는 역할을 수행한다.

그리고, 상기 관리 프로세서(134)는 상기와 같은 각 프로세서가 각각의 고유 작업을 동시 다발적으로 수행될 수 있도록 관리하고 운영하는 역할을 수행한다.

이와 함께, 본 발명에서는 전술한 바와 같은 IDS 커널(130)이 MDB(160)에 저장된 각 패킷의 이상 유무에 따른 정보를 토대로 선택적인 경고를 발생시키도록 프로세싱되는 경고 프로세서(Alert Processor)(135)와, 상기 MDB(160)에 저장된 각 데이터 패킷의 이상 유무에 따른 정보를 토대로 침입된 경로를 역추적하는 추적 프로세서(Chase Processor)(136), 상기 MDB(160)의 저장 공간을 지속적으로 확인하고, 상기 저장 공간이 기 설정된 저장 공간에 비해 부족할 경우 추가되는 데이터 패킷 혹은, 처리 완료된 데이터 패킷을 별도의 하드웨어 저장 공간에 저장하는 로깅 프로세서(Logging Processor)(137) 그리고, 정상적인 패킷으로 판단된 데이터 패킷만을 전송 대상 컴퓨터 시스템으로 전송하는 패킷 전송 프로세서(Gateway Processor)(138)를 더 포함하여 모듈화됨을 제시한다.

이 때, 상기 별도의 하드웨어 저장 공간이라 함은 통상적인 HDD(180)가 될 수 있다.

도시한 도 3은 전술한 바와 같은 IDS 커널과 메모리 데이터 베이스간 연동을 위해 설정된 상태에 따른 구성도를 나타내고 있다.

뿐만 아니라 본 발명에 따른 네트워크 보호 시스템을 구성하는 침입 탐지 시스템(100)에는 각 데이터 패킷의 비정상적인 동작 발생에 대응하여 상기 시스템을 관리하는 관리자가 수동 조작할 수 있도록 하기 위한 유저 인터페이스(UI: User Interface)(190)가 더 포함되어 구축됨을 제시한다.

이 때, 상기 UI는 IDS 커널(130)의 동작 상태를 디스플레이하고, 관리자로부터의 조작 신호를 수신 받기 위한 응용 프로그램이 된다.

이하, 전술한 바와 같은 본 발명의 네트워크 보호 시스템을 이용한 네트워크 보호 방법을 첨부된 도 4의 내지 도 8의 순서도를 참조하여 보다 구체적으로 설명하기로 한다.

우선, 본 발명의 네트워크 보호 시스템을 구성하는 허브(200)는 인터넷 망 혹은, 인트라넷 망을 통해 특정 컴퓨터 시스템으로부터의 접속 요청 데이터 신호, 혹은 데이터 전송에 따른 신호를 입수 받음과 함께 상기 신호의 수신 대상 컴퓨터 시스템(300)을 확인하여 해당 컴퓨터 시스템이 포함되어 구축된 네트워크로 상기 입수된 데이터 신호를 전달한다.

이와 함께, 본 발명의 침입 탐지 시스템(100)은 상기 허브(200)와 네트워크 사이의 데이터 전달 경로 상에 설치된 상태로써 NIC(150)를 통해 상기 데이터가 전달되는 경로와의 세션 연결을 이룬다.(S110)

이후, 상기 침입 탐지 시스템(100)은 상기 세션을 통해 전달되는 데이터 패킷을 수신하게 된다.(S120)

이 때, 침입 탐지 시스템(100)을 구성하는 인터럽트부(120)는 상기 NIC(150)를 통한 데이터 수신 여부에 따른 인터럽트 신호를 계속하여 판독하고 있는 상태임에 따라 상기 NIC(150)를 통해 데이터가 수신될 경우 이의 인터럽트 신호를 판독한 후 IDS 커널(130)로 상기 수신되는 데이터 패킷을 전달한다.(S130)

그리고, 상기 IDS 커널(130)은 상기 수신되는 데이터 패킷을 MDB(160)에 저장함과 더불어 상기 MDB(160)와 연동하면서 해당 데이터 패킷의 이상 여부에 따른 확인 및 그 방어를 수행한다.(S140)

이 과정에서 IDS 커널(130)은 상기 수신되는 데이터 패킷에 이상이 있을 경우 전송 대상 컴퓨터 시스템(300)으로의 전달됨을 불허함과 동시에 그 내역을 저장(S150)해 둔 후 세션 연결을 해제(S160)하여 더 이상의 데이터 패킷 전송을 차단한다.

반면, 상기 수신되는 데이터 패킷에 이상이 없을 경우 해당 데이터 패킷의 전송을 허용함과 동시에 그 내역을 저장(S170)하고, 상기 전송 대상 컴퓨터 시스템(300)으로의 전달을 수행한다.(S180)

이 때, 상기한 IDS 커널(130)과 MDB 상호간 연동에 의한 침입 탐지 및 대응 과정을 도시한 도 5 내지 도 10의 순서도를 참고하여 보다 구체적으로 설명하도록 한다.

우선, 도시한 도 5의 순서도와 같이 NIC(150) 및 인터럽트부(120)를 통해 IDS 커널(130)로의 데이터 패킷이 수신되면 상기 IDS 커널(130)은 패킷 수집 프로세서(131)를 통해 데이터 패킷을 지속적으로 수집하여 MDB(160)로 전달함으로써 상기 MDB(160)에 해당 데이터 패킷의 저장이 이루어지도록 한다.(S141)

이 때, 상기 패킷 수집 프로세서는 수신된 데이터를 프로토콜(Protocol), 세션(Session), 서버(Server), 클라이언트(Client) 등과 같은 각종 정보로써 각각 분리한 후 MDB(160)에 저장하게 된다.

이와 동시에 상기 IDS 커널(130)은 관리 프로세서(134)를 통해 분석 프로세서(132), 방어 프로세서(133), 추적 프로세서(136), 로깅 프로세서(137), 경고 프로세서(135) 그리고, 패킷 전송 프로세서(138)를 동시에 다발적으로 수행시켜 상기 MDB(160)에 저장된 각 데이터 패킷의 이상 유무 확인 및 그에 따른 처리를 수행한다.

이 때, 상기 분석 프로세서(132)를 통해서 도시한 도 6의 순서도와 같이 MDB(160)에 저장되어 있는 각 데이터 패킷을 분석하여 그 이상 유무를 판독하고, 그 결과 정보를 상기 MDB(160)에 재저장한다.

상기에서 분석 프로세서에 의한 데이터 패킷의 이상 유무 확인은 상기 MDB에 이미 등록되어 있는 정상적인 데이터 패킷의 유형에 대한 정보 혹은, 비정상적인 데이터 패킷의 유형에 대한 정보를 토대로 수행하게 된다.

이 때, 상기 비정상적인 데이터 패킷의 유형에 대한 정보의 예로는 각종 바이러스 감염 여부, 사용자 데이터그램 프로토콜을 이용한 동일 데이터의 반복적인 전송 여부(UDP Flooding 공격 여부), 핑(Ping) 명령어가 기 설정된 소정 횟수(예컨대, 30회) 이상 수신되는지에 대한 여부(Ping Flooding 공격 여부), 프로그램을 이용한 대량 메일이 전송되어지는지에 대한 여부(Mail Bomb 공격 여부), 파일전송프로토콜(FTP) 데이터 패킷이 1024번 아래의 포트를 오픈하도록 설정되어 있는지에 대한 여부(FTP Port Bound 공격 여부), 권한 밖의 명령어(Write, Delete 등)를 실행하도록 이루어져 있는지에 대한 여부(FTP Violation 공격 여부), 웹 서비스(Web service)나 텔넷 서비스(Telnet service)나 파일전송프로토콜 서비스(FTP service) 등과 같은 서비스 프로그램에서 처리할 수 있는 문자열 보다 많은 문자열이 포함되어 있는지에 대한 여부(Buffer Overflow 공격 여부), 기 등록된 라우터의 하드웨어 주소(MAC Address)와 전송되는 TCP/IP의 하드웨어 주소간 동일성 여부(IP Spoofing 공격 여부), 핑거 명령어(Finger)의 포함 여부(Finger 공격 여부) 등이 있을 수 있는데, 반드시 이로만 한정되지 않으며 보다 다양하게 있을 수 있다.

그리고, 상기한 내역을 토대로한 분석 프로세서(132)에 의한 데이터 패킷의 이상 유무에 따른 확인 결과는 MDB(160)에 저장한다.

즉, 정상적인 유형의 데이터 패킷으로 판단될 경우 그 결과 정보를 MDB(160)에 저장하게 되고, 비 정상적인 유형의 데이터 패킷으로 판단될 경우 그 결과 정보 및 해당 유형을 상기 MDB(160)에 저장하는 것이다. 이와 함께 상기 분석 프로세서는 계속해서 상기 MDB(160)에 저장되어 있는 또 다른 데이터 패킷의 이상 유무에 대한 확인을 수행하게 된다.

또한, 방어 프로세서(133)를 통해서 도시한 도 7의 순서도와 같이 상기 MDB(160)에 저장되어 있는 각 이상 발생 데이터 패킷의 이상 발생 유형에 따른 처리를 수행하게 된다.

예컨대, 각종 바이러스를 가지는 데이터 패킷일 경우 바이러스 백신 소프트웨어를 구동하여 그 치료를 수행하고, 상기 치료 완료된 데이터 패킷은 정상적인 데이터 패킷으로 재 설정하여 MDB(160)에 저장한다. 이 때, 상기 백신 소프트웨어에 의한 치료 수행이 불가능할 경우 해당 데이터 패킷의 삭제를 수행함과 더불어 더 이상의 전송됨을 차단한다.

하지만 반드시 이의 방법에 의해 수행됨으로 한정하지는 않으며, 치료의 수행 없이 해당 데이터 패킷의 삭제 및 더 이상의 전송됨을 차단하도록 설정할 수도 있다.

만일, 이상 발생 유형이 각종 해커에 의한 공격일 경우 MDB(160)에 기 등록되어 있는 각종 해킹 유형별 대응 방법에 따라 그 대처(예컨대, 해당 데이터 패킷의 삭제 및 해당 세션 차단)를 수행하고, 바이러스 및 해커 침입이 아닌 통상적인 오류 데이터일 경우 설정된 대처 방법(예컨대, 반송 등)에 따른 대처를 수행한다.

또한, 상기의 과정이 진행되는 도중 IDS 커널(130)의 추적 프로세서(136)는 도시한 도 8의 순서도와 같이 MDB(160)에 저장되는 각 데이터 패킷의 이상 발생 여부를 지속적으로 확인하다가 해커의 침입에 따른 데이터 패킷의 이상 발생이 확인될 경우 해당 데이터 패킷의 침입 경로 및 최초 송신지에 대한 추적을 수행하게 된다.

이 때, 상기 추적 프로세서(136)의 의한 침입 경로의 추적은 해당 데이터 패킷의 분석 정보가 저장된 MDB(160)를 통해 송신 컴퓨터 시스템에 대한 IP(Internet Protocol)를 확인한 후 최근 상기 IP에 세션 연결되었던 각 컴퓨터 시스템 중 이상이 발생된 데이터 패킷과 동일한 데이터 패킷을 수신한 컴퓨터 시스템의 IP를 확인한다.

이의 과정은 해당 데이터 패킷의 수신에 이루어지지 않았지만 그 송신은 이루어졌었던 컴퓨터 시스템의 IP가 확인될 때까지 반복적으로 수행함과 동시에 상기 이상 발생 데이터 패킷의 발생 확인 시간으로부터 인접한 시각의 범위 내에 각 데이터 패킷을 송수신하였던 각 컴퓨터 시스템을 확인함으로써 수행된다.

그리고, 상기한 과정에 의해 확인된 IP가 해킹 시도한 IP로 판단하여 그 내역을 저장함과 동시에 현재 상기 IP에 세션 연결된 여타 컴퓨터 시스템과의 세션 차단을 수행한다.

이 때, 본 발명에서는 상기한 과정이 가능할 수 있도록 각 컴퓨터 시스템간 세션 연결을 통해 수행된 데이터 패킷의 전송 내역이 시간대 별로 소팅(sorting)하여 저장함을 추가로 제시한다.

그리고, 상기의 과정을 통해 확인된 최종 컴퓨터 시스템이 해당 이상 발생 데이터 패킷의 전송 시발점으로 판단함과 더불어 그 IP를 취득하여 침입 경로와 함께 MDB(160)에 저장한다.

또한, 상기한 과정에서 IDS 커널(130)의 경고 프로세서(135)는 도시한 도 9의 순서도와 같이 상기 각 프로세서(131, 132, 133, 134, 136, 137)의 동작됨과 동시에 MDB(160)에 저장되는 각 데이터 패킷의 이상 발생 여부를 지속적으로 확인하게 되며, 이의 과정 중 특정 데이터 패킷의 이상 발생이 확인될 경우 해당 네트워크를 관리하는 관리자에게 상기 이상 발생에 따른 내역을 통보함으로써 관리자에 의한 직접적인 관리가 가능하도록 한다.

이 때, 상기 관리자로의 통보는 IDS 커널(130)의 경고 프로세서(135)가 MDB(160)에 저장된 이상 발생 데이터 패킷에 대한 내역, 침입한 컴퓨터 시스템의 정보, 침입 유형 등과 같은 각종 정보를 유저 인터페이스(User Interface)(190)로 송신하고, 상기 UI(190)에서는 상기 수신된 정보를 해당 관리자의 컴퓨터 시스템 화면상에 디스플레이함으로써 가능하다.

상기에서 UI(190)는 상술한 바와 같이 IDS 커널(130)의 경고 프로세서(135)를 통해 확인된 이상 발생 데이터 패킷의 내역만을 해당 관리자에게 통보하는 역할을 수행하는 것은 아니다. 각종 데이터 패킷의 전송 현황이나 이상 발생 데이터 패킷의 유형 및 그 처리 결과 등에 대한 정보도 함께 통보할 수 있도록 MDB(160) 및 IDS 커널(130)로부터 해당 정보를 전달받도록 설정함이 보다 바람직하다.

또한, 전술한 바와 같은 각 과정이 진행되는 도중 IDS 커널(130)의 로깅 프로세서(137)는 도시한 도 10과 같이 MDB(160)의 저장 상태를 지속적으로 확인함과 더불어 상기 MDB(160)이 기 설정된 허용 저장 용량을 초과하였을 경우 상기 MDB(160)로 저장되는 각종 데이터 패킷을 별도의 하드웨어 저장 공간인 HDD(180)에 분산 저장하는 역할을 수행한다.

이 때, 상기 별도의 하드웨어 저장 공간에는 IDS 커널(130)의 각 프로세서(131, 132, 133, 134, 135, 136, 137)와 MDB(160) 상호간의 연동에 따른 침입 탐지 결과에 대한 각종 내역 정보가 지속적으로 등록될 수 있도록 한다.

이는, 상기 MDB(160)가 가지는 저장 공간 상의 한계를 고려함과 더불어 침입 탐지를 위해 IDS 커널(130)과 연동하면서 계속적인 동작을 수행하는 MDB(160)의 부하에 따른 부담을 저감시킬 수 있도록 하기 위함이다.

즉, 해당 네트워크의 관리자가 유저 인터페이스(190)를 통한 각종 침입 탐지 동작 내역에 대한 조회를 수행할 경우 별도의 데이터 저장을 위한 하드웨어를 통해 해당 정보가 취득될 수 있도록 함으로써 MDB(160)에 대한 저장 공간 상의 부담 및 부하 증가에 따른 부담이 해소될 수 있도록 함을 제시하는 것이다. 물론, MDB에 상기 침입 탐지의 결과 내역을 저장할 수도 있음은 당연하다.

또한, 전술한 바와 같은 각 과정이 진행되는 도중 IDS 커널(130)의 패킷 전송 프로세서(138)는 전술한 바와 같은 IDS 커널(130)의 각 프로세서(131, 132, 133, 134, 135, 136, 137) 및 MDB(160) 상호간 연동을 통해 수신되는 데이터 패킷에 대한 이상 여부 확인 결과 이상이 없음으로 확인된 데이터 패킷만을 인터럽트부(120) 및 NIC(150)를 각각 통과하여 해당 데이터의 전송 대상 컴퓨터 시스템(300)으로 전달된다.

이 때, 상기 이상이 없는 데이터 패킷의 전달은 최초 IDS 커널(130)로의 데이터 패킷 전달 과정에 대하여 역순으로 이루어진다.

즉, IDS 커널(130)로부터 이상이 없는 데이터 패킷이 인터럽트부(120) 및 NIC(150)로 순차적인 전달이 이루어짐과 더불어 상기 NIC(150)를 통해 전송 대상 컴퓨터 시스템(300)이 구축된 네트워크의 허브(혹은, 전송 대상 컴퓨터 시스템)(200)로 전달되는 것이다.

물론, 해당 데이터 패킷에 이상이 있음으로 확인되었을 경우에는 기 전술한 바와 같이 방화 프로세서(133)와 연동하여 해당 데이터 패킷을 송신한 송신측 컴퓨터 시스템과의 접속 세션을 차단함으로써 더 이상의 데이터 패킷 전송이

이루어지지 않도록 조치된다.

결국, 전술한 각 과정의 순차적이고 반복적인 수행에 의해 소정의 네트워크를 이루는 컴퓨터 시스템은 바이러스 및 해킹 등으로부터 보호됨이 가능해진다.

발명의 효과

이상에서 설명한 바와 같이 본 발명에 따른 네트워크 보호 시스템 및 그 운영 방법은 침입 탐지를 위한 엔진을 모듈화된 커널로써 구현함에 따라 그 처리를 위한 경로가 단축되어 보다 우수한 처리 시간의 단축을 이룰 수 있게 된 효과가 있다.

뿐만 아니라, 상기와 같은 데이터 패킷의 흐름 경로가 단축됨에 따른 데이터 손실이 저감되어 해당 데이터의 훼손을 방지할 수 있게 된 효과 역시 있다.

또한, 커널을 침입 탐지 엔진으로 구현함과 더불어 각 데이터의 흐름 경로상에 설치함으로써 전송 대상 컴퓨터 시스템으로의 해당 이상 발생 데이터의 전송이 이루어지기 전에 상기 이상 발생 데이터의 차단 수행이 가능해짐에 따라 각종 해킹 공격에 대한 방어가 보다 완전하게 수행될 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1.

인터넷 망을 통해 연결된 특정 영역 외부에 구축된 네트워크의 컴퓨터 시스템 및 특정 영역 내부에 구축된 네트워크의 특정 컴퓨터 시스템 혹은, 특정 영역 내부에 구축된 네트워크의 각 컴퓨터 시스템간 데이터 전달을 위해 설치된 최소 하나 이상의 허브;

상기 특정 영역 내부에 구축된 네트워크망을 이루며, 각 허브에 접속된 상태로써 네트워크 가능하게 연결된 다수의 서버 컴퓨터 시스템 및 개인용 컴퓨터 시스템;

상기 각 허브 중 어느 한 허브와 이 허브에 연결된 다른 한 허브 혹은, 컴퓨터 시스템과의 데이터 전달 경로 사이에 최소 하나 이상 설치되며, 상기 데이터 전달 경로 사이의 데이터 전달에 대한 인터럽트 신호를 수신받아 침입 탐지 및 방어를 수행하도록 침입 탐지 엔진이 모듈화되어 이루어진 커널(kernel)을 가지는 침입 탐지 시스템(IDS; Intrusion Detection System);을 포함하여 구축된 네트워크 보호 시스템.

청구항 2.

제 1 항에 있어서,

침입 탐지 시스템은 침입 탐지 및 방어를 수행하도록 모듈화된 커널과 더불어 데이터 송수신을 위한 네트워크 인터페이스 카드(NIC; Network Interface Card)를 가지고,

상기 네트워크 인터페이스 카드를 통한 데이터의 수신 여부에 따른 인터럽트 신호를 판독하기 위한 인터럽트부를 가지며,

상기 모듈화된 커널을 통해 수신되는 각 데이터 패킷을 임시 저장하고, 각 패킷의 이상 현상에 대한 정보 및 각 패킷의 이상 상태별 대응 방법에 대한 제어 정보가 각각 저장되는 메모리 데이터 베이스(Memory Data Base)를 가지고,

상기 각 구성 부분간의 데이터 전송이 이루어지도록 연결된 데이터 버스(Data Bus)를 가짐을 특징으로 하는 네트워크 보호 시스템.

청구항 3.

제 2 항에 있어서,

모듈화된 커널은

인터럽트부를 통해 데이터의 수신 여부가 확인될 경우 해당 데이터 패킷을 지속적으로 받아들이며 메모리 데이터 베이스에 저장하는 패킷 수집 프로세서(Gathering Processor)와,

상기 메모리 데이터 베이스에 저장되어 있는 각 데이터 패킷을 분석하여 그 이상 유무를 판독하고, 그 결과 정보를 상기 메모리 데이터 베이스에 저장하는 분석 프로세서(Analyze Processor)와,

상기 메모리 데이터 베이스에 저장된 각 패킷의 이상 유무에 따른 정보를 토대로 선택적인 방어를 수행하는 방어 프로세서(Defense Processor)와,

상기한 각 프로세서의 다중 제어(Multi processor)를 관리하기 위한 관리 프로세서(Manager Processor)와,

상기 메모리 데이터 베이스에 저장되는 각 패킷 중 그 이상이 없음으로 확인되었거나 치유가 완료된 데이터 패킷을 전송 대상 컴퓨터 시스템으로 전달하기 위한 패킷 전송 프로세서(Gateway Processor)를 포함하여 설정됨을 특징으로 하는 네트워크 보호 시스템.

청구항 4.

제 3 항에 있어서,

모듈화된 커널에는

메모리 데이터 베이스에 저장된 각 패킷의 이상 유무에 따른 정보를 토대로 선택적인 경고를 발생시키는 경고 프로세서(Alert Processor)가 더 포함되어 설정됨을 특징으로 하는 네트워크 보호 시스템.

청구항 5.

제 3 항에 있어서,

모듈화된 커널에는

메모리 데이터 베이스에 저장된 각 패킷의 이상 유무에 따른 정보를 토대로 침입 경로를 추적하는 추적 프로세서(Chase Processor)가 더 포함되어 설정됨을 특징으로 하는 네트워크 보호 시스템.

청구항 6.

제 3 항에 있어서,

모듈화된 커널에는

메모리 데이터 베이스의 저장 공간을 지속적으로 확인하고, 상기 저장 공간 이 기 설정된 저장 공간에 비해 부족할 경우 추가되는 데이터 패킷 혹은, 처리 완료된 데이터 패킷을 별도의 하드웨어 저장 공간에 저장하는 로깅 프로세서(Logging Processor)가 더 포함되어 설정됨을 특징으로 하는 네트워크 보호 시스템.

청구항 7.

제 2 항에 있어서,

침입 탐지 시스템에는

각 데이터 패킷의 비정상적인 동작 발생에 대응하여 관리자가 수동 조작할 수 있도록 하기 위한 유저 인터페이스(User Interface)가 더 포함되어 구축됨을 특징으로 하는 네트워크 보호 시스템.

청구항 8.

인터럽트부를 이용한 인터럽트 신호의 수신을 통해 각 컴퓨터 시스템간 세션 연결의 요청 여부를 지속적으로 확인하는 제1단계;

상기 과정에서 특정 컴퓨터 시스템으로부터 다른 한 컴퓨터 시스템으로의 세션 연결을 위한 요청 신호가 발생될 경우 이 세션을 통해 전송되는 데이터 패킷을 커널로 전달하도록 제어하는 제2단계;

상기 커널을 메모리 데이터 베이스와 연동시켜 수신된 데이터 패킷의 이상 유무를 판독함과 더불어 그 판독 결과에 따라 전송 대상 컴퓨터 시스템으로의 해당 데이터 패킷 전송 혹은, 차단을 결정하며, 상기 결정에 따른 제어를 수행하는 제3단계:가 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 9.

제 8 항에 있어서,

제2단계가 수행되는 과정에서 데이터 패킷을 커널로 전달하는 과정은

세션 연결을 요청한 특정 컴퓨터 시스템과 침입 탐지 시스템을 구성하는 네트워크 인터페이스 카드 상호간의 세션을 연결하는 단계;

상기 연결된 세션을 통해 데이터 패킷을 수신 받는 단계;

상기 네트워크 인터페이스 카드를 통해 수신된 데이터 패킷을 커널로 연속하여 전달하는 단계;가 순차적으로 수행되어 이루어짐을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 10.

제 8 항에 있어서,

제3단계의 운영 과정은

커널의 패킷 수집 프로세서를 구동하여 데이터 패킷을 지속적으로 수신함과 더불어 이 수신한 데이터 패킷을 메모리 데이터 베이스에 저장하는 단계;

상기 커널의 분석 프로세서를 구동하여 메모리 데이터 베이스에 저장되는 각 데이터 패킷을 분석함으로써 그 이상 유무를 판독하고, 그 결과 정보를 메모리 데이터 베이스에 재저장하는 단계;

상기 메모리 데이터 베이스에 저장된 특정 데이터 패킷의 이상 발생이 확인될 경우 상기 커널의 방어 프로세서를 구동하여 해당 데이터 패킷의 전달 취소를 수행하고, 상기 메모리 데이터 베이스에 저장된 특정 데이터 패킷의 이상 발생이 확인되지 않을 경우에는 패킷 전송 프로세서를 통해 해당 데이터 패킷을 전송 대상 컴퓨터 시스템으로 전달하는 단계;가 각각 포함되어 운영됨으로써 수행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 11.

제 10 항에 있어서,

각 프로세서의 구동은 관리 프로세서를 통해 동시적인 작업이 수행될 수 있도록 제어됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 12.

제 10 항에 있어서,

데이터 패킷을 메모리 데이터 베이스에 저장하기 전 상기 데이터 패킷을 프로토콜(Protocol), 세션(Session), 서버(Server), 클라이언트(Client) 등의 정보로 각각 분리하는 단계가 더 포함되어 운영됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 13.

제 10 항에 있어서,

데이터 패킷의 분석 과정 중 그 이상 유무를 판독하기 위해

해당 데이터 패킷이 메모리 데이터 베이스에 기록되어 있는 각종 바이러스에 감염된 데이터 유형인지를 비교 검색하는 단계;

상기 비교 검색 결과 해당 데이터 패킷이 바이러스에 감염된 데이터 유형임으로 확인될 경우 해당 데이터 패킷에 이상이 있음으로 판독하는 단계;가 더 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 14.

제 10 항에 있어서,

데이터 패킷의 분석 과정 중 그 이상 유무를 판독하기 위해

해당 데이터 패킷이 메모리 데이터 베이스에 설정되어 있는 각 해킹 패턴에 따른 데이터 유형인지를 비교 검색하는 단계;

상기 비교 검색 결과 해당 데이터 패킷이 기 설정된 최소 어느 하나의 해킹 패턴에 따른 데이터 유형임으로 확인될 경우 해당 데이터 패킷에 이상이 있음으로 판독하는 단계:가 더 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 15.

제 10 항에 있어서,

데이터 패킷의 분석 과정 중 그 이상 유무를 판독하기 위해

해당 데이터 패킷이 메모리 데이터 베이스에 설정되어 있는 차단 대상 데이터 유형인지를 비교 검색하는 단계;

상기 비교 검색 결과 해당 데이터 패킷이 기 설정된 최소 어느 하나의 차단 대상 데이터 유형임으로 확인될 경우 해당 데이터 패킷에 이상이 있음으로 판독하는 단계:가 더 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 16.

제 15 항에 있어서,

차단 대상 데이터 유형이라 함은

비인가된 사이트로의 접속을 위한 데이터, 권한을 가지고 있지 않은 어느 한 컴퓨터 시스템으로의 접속을 위한 데이터 중 최소 어느 하나를 포함하는 유형임을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 17.

제 10 항에 있어서,

메모리 데이터 베이스에 저장된 특정 데이터 패킷의 이상 발생이 확인될 경우

커널의 경고 프로세서를 통해 침입 탐지 시스템의 유저 인터페이스로 상기 이상 발생 내역을 전송함으로써 해당 시스템의 관리자에게 통보될 수 있도록 하는 단계가 더 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 18.

제 10 항에 있어서,

메모리 데이터 베이스에 저장된 특정 데이터 패킷의 이상 발생이 확인될 경우

커널의 방어 프로세서를 통해 상기 패킷의 이상 유무에 따른 정보를 토대로 선택적인 방어를 수행하는 단계가 더 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 19.

제 18 항에 있어서,

방어 프로세서가 수행하는 방어 과정은

이상 발생 데이터 패킷의 송신측 컴퓨터 시스템과의 연결 세션을 차단하여 더 이상의 전송됨을 방지함과 더불어 메모리 데이터 베이스에 저장된 해당 데이터 패킷의 삭제를 수행함으로써 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 20.

제 10 항에 있어서,

메모리 데이터 베이스에 저장된 특정 데이터 패킷의 이상 발생이 확인될 경우

커널의 추적 프로세서를 통해 침입 경로를 추적하는 단계가 더 포함되어 진행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 21.

제 20 항에 있어서,

추적 프로세서를 이용한 침입 경로의 추적 방법은

데이터 패킷의 송신 컴퓨터 시스템에 대한 IP(Internet Protocol)를 확인하는 단계;

최근 상기 확인된 컴퓨터 시스템의 IP에 세션 연결되었던 각 컴퓨터 시스템 중 이상이 발생된 데이터 패킷과 동일한 데이터 패킷을 전송하였던 컴퓨터 시스템의 IP를 확인하는 과정을 반복 수행하여 해당 데이터 패킷의 전송 시발점 IP를 확인하는 단계가 포함되어 진행됨으로써 수행됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 22.

제 21 항에 있어서,

이상 발생 데이터 패킷과 동일한 데이터 패킷을 전송하였던 컴퓨터 시스템의 IP를 확인하기 위해

각 컴퓨터 시스템간 세션 연결을 통해 수행된 데이터 패킷의 전송 내역을 그 시간별로 지속적인 저장을 수행하는 단계가 더 포함되어 운영됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

청구항 23.

제 10 항에 있어서,

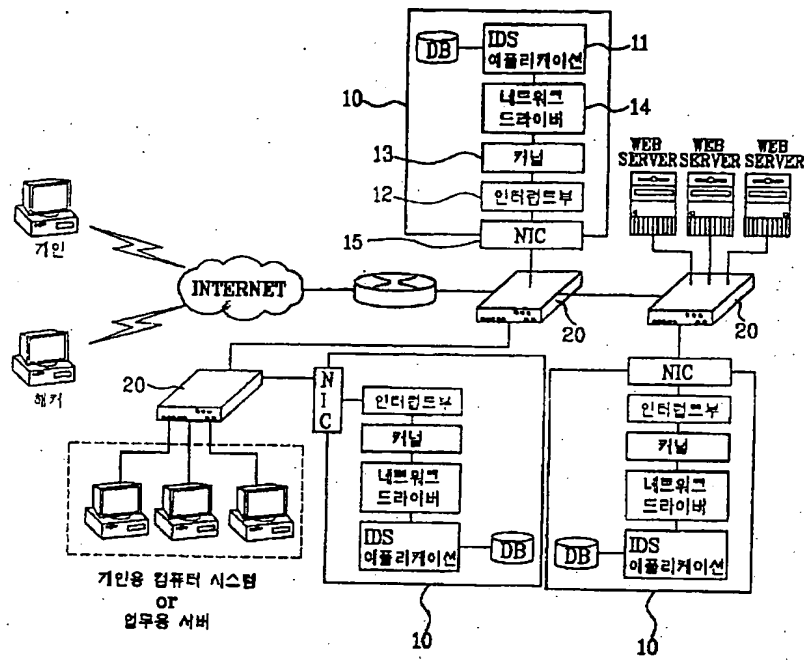
각 프로세서의 동작이 수행되는 도중 커널의 로깅 프로세서(Logging Processor)는

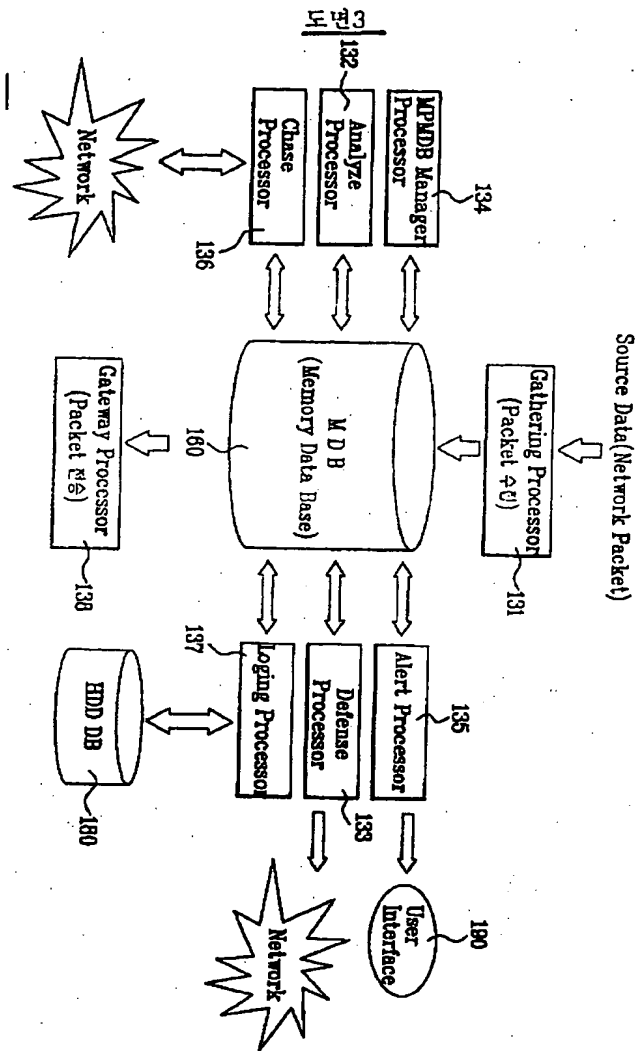
메모리 데이터 베이스의 저장 공간을 지속적으로 확인하는 단계;

상기 단계의 확인 결과 그 저장 공간이 기 설정된 저장 공간에 비해 부족함으로 판단될 경우 추가되는 데이터 패킷 혹은, 처리 완료된 데이터 패킷을 별도의 하드웨어 저장 공간에 저장하는 단계를 포함하여 운영됨을 특징으로 하는 네트워크 보호 시스템의 운영 방법.

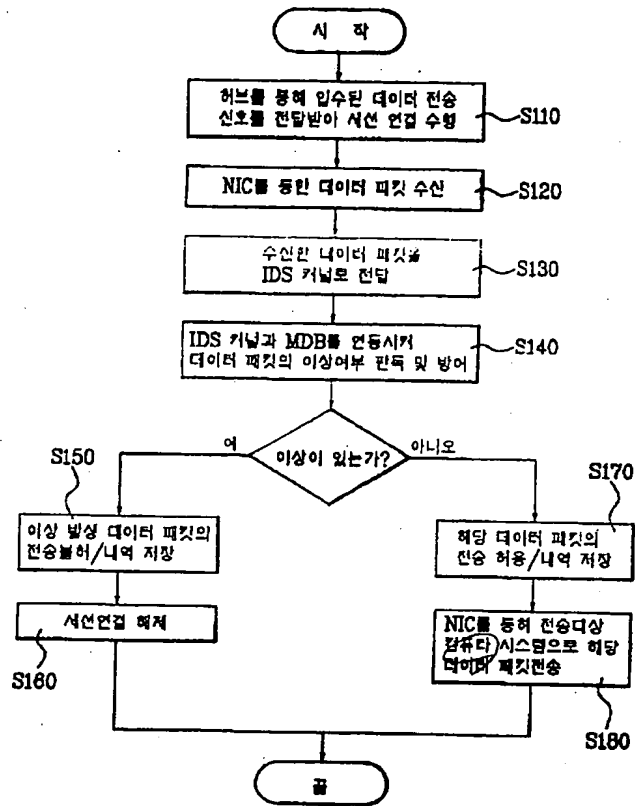
도면

도면1

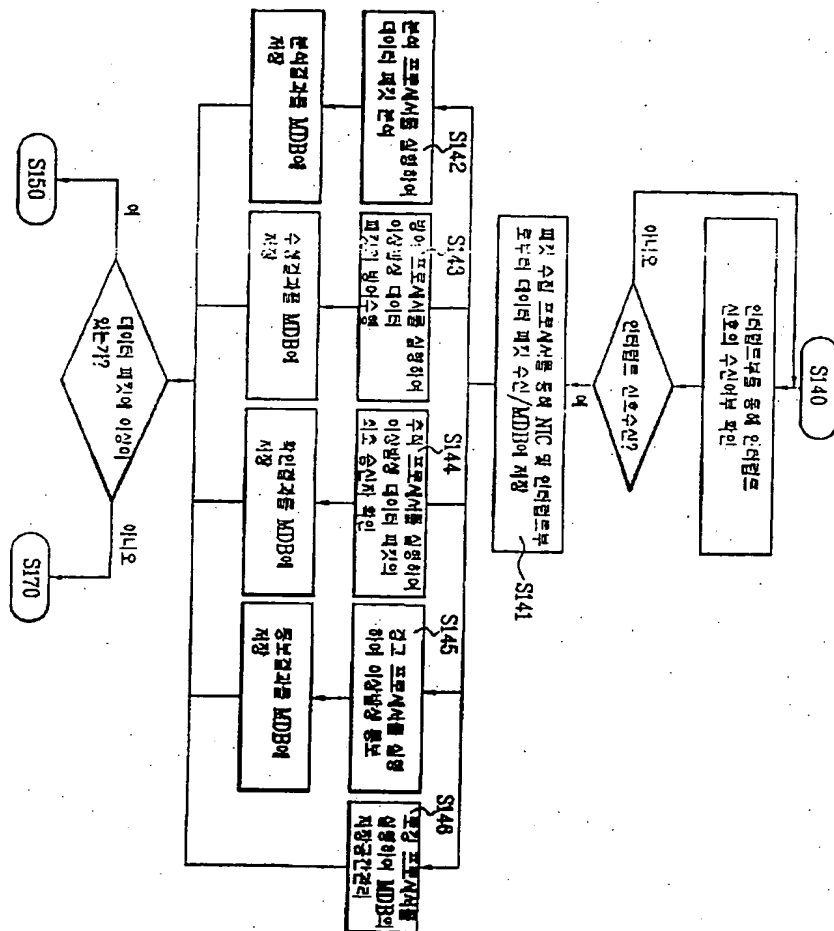




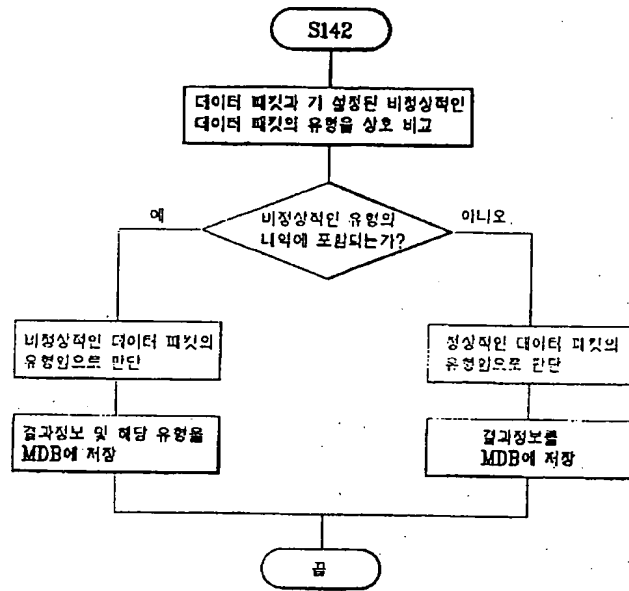
도면4



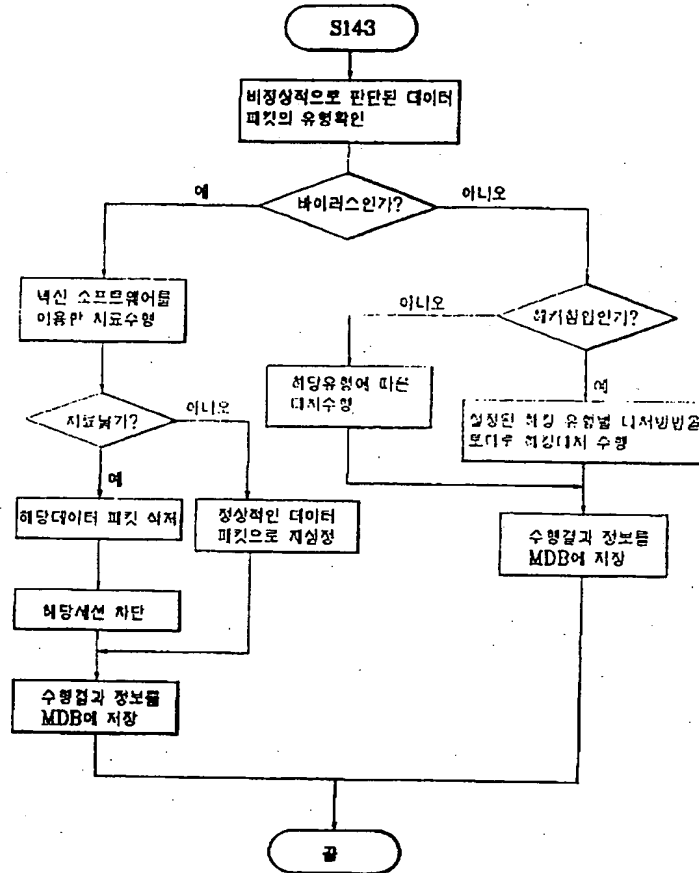
도면5



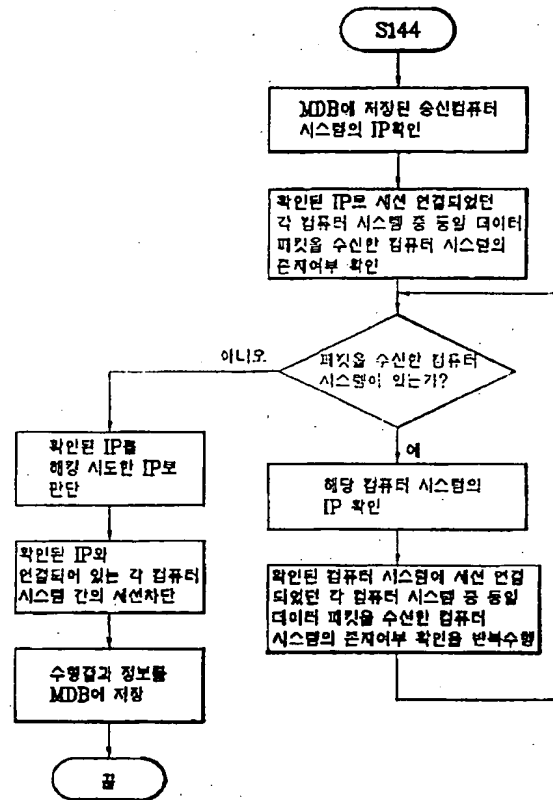
도면6



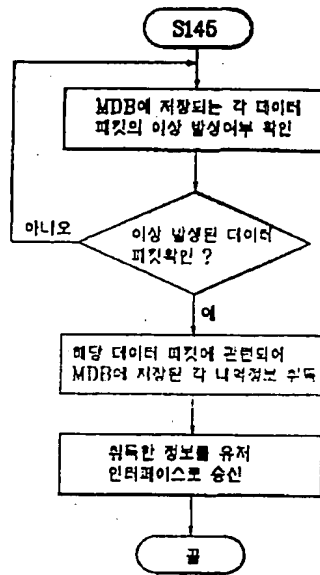
도면7



도면8



도면9



도면10

